REMARKS

Applicant would like to thank the Examiner for extending the courtesy of a telephone interview on July 26, 2005. The parties to the interview consisted of Mathew T. Henning, the Examiner responsible for examination of the present patent application, and Manisha Chakrabarti (Registration No. 41,665), attorney for the Applicant. The interview focused on amendments to independent claims 1, 21, 23 to distinguish over the teachings of Cellier et al (U.S. Patent No. 5,884,269). Amendments to independent claims 1, 21 and 23 and arguments in support of all such amendments are presented below and reflect discussions with the Examiner. Applicant has filed a Request for Continued Examination so that further searches may be conducted if deemed warranted by the Examiner.

Claims 1-3, 5-10 and 21-61 stand rejected in the present application. Claims 1, 2, 21, 23, 33, 34, 37-39, 42, 43, 48, 52-54, 57, and 58, have been amended by way of this amendment. Claims 1-3, 5-10, 21-61 are currently pending and at issue in the present application.

The drawings have been objected to for failing to show every feature of the invention specified in the claims. Claims 38 and 53 have been amended. The feature of the invention recited in claims 38 and 53 is a component of the "Data Analysis" referred to as reference numeral 130 on FIG. 1 of the drawings. Amended claims 39 and 54 further detail the "Relationship Analysis" referred to as reference numeral 134 on FIG. 2 of the drawings.

With respect to the objections relating to claims 41, 42, 56, and 57, FIG. 2 has been corrected to include the step 165 "Apply Additional Encryption" thereby providing

support for encrypting the encrypted data string as recited by the claims 41, 42, 56 and 57. Support for the drawing change can be found in the specification on page 11, lines 18 through page 12, line 7 under in the heading "Additional Encryption." No new matter has been entered by virtue of the changes to the drawings.

A Replacement Sheet and a prior version of the drawing sheet including FIG. 2 has been submitted in accordance with 37 CFR 1.121(d) for consideration by the Examiner.

Since the features of the invention recited in the amended claims 38, 53, 39, 54 are shown in the drawings and FIG 2 has been corrected to illustrate the features of the invention recited in claims 41, 42, 56 and 57, the objection to the drawings as failing to show every feature of the invention recited in the claims at issue should be withdrawn.

The specification is objected to as failing to provide antecedent basis for the claims 34, 37-39, 48, and 52-54. Claims 34, 37, 39-40, 48, 52, 54-55 have been rejected under 35 U.S.C. §112, first paragraph as failing to comply with the written description requirement.

Claims 34 and 48 have been amended to comply with the written description requirement. Support for amended claims 34 and 48 can be found on page 18 lines 17 of the specification. More specifically, the specification states that "Alternatively, the control code can be generated in a random or non-random..." Accordingly the rejection of claims 34 and 48 as failing to comply with the written description should be withdrawn.

Claims 37, 39, 52 and 54 have been amended to comply with the written description requirement. Support for amended claims 37, 39, 52, and 54 can be found in

the section beginning on page 5 of the specification with the heading "Section C Data Analysis." More specifically, page 5, lines 17 of the specification states:

> "The data within each block 22, 24 is analyzed to determine whether certain characteristics exist within the data. In response to the presence or absence of these characteristics, the step of generating the position code (step 150) can be altered, as described below, so that the input data string 20 can be compressed simulateously as it is encrypted."

The section goes on to describe the specifics of the analysis of the relationship between the groups of n bits within in the input data. Since support for the amended claims 37, 39, 52 and 54 is present in the specification, the rejection of claims 37, 39, 52, 54 and claims 40 and 55 depending from claims 39 and 54, respectively, should be withdrawn.

Claim 52 has been objected to for containing a number of typographical errors. Claim 52 has been amended to correct all such errors, accordingly the objection to claim 52 should be withdrawn.

Claim 2 has been rejected under 35 U.S.C. §112, second paragraph for failing to provide sufficient antecedent basis. Claim 2 has been amended to provide sufficient antecedent basis. Accordingly, the rejection of claim 2 as being indefinite should be withdrawn.

Independent claim 1 and claims 2, 3, 5, 8-10, 47, 49-52, 53-55 and 59-61 dependent thereon, stand rejected under 35 U.S.C. §102(b) as anticipated by Cellier et al (U.S. Patent No. 5,884,269). Independent claim 21 and claim 22 dependent thereon, as well as independent claim 23 and claims 24-26, 29-33, 35-37, 38-40 and 44-46 dependent

thereon, stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cellier et al. in view of the Schneier "Applied Cryptography" publication.

Amended independent claims 1, 21 and 23, recite methods and a computer usable medium storing a computer program for encrypting an input data string. An order is determined for querying the presence of each of 2^n different configurations of n bits within the input data string. A control code that is associated with the determined order is generated. A position code is generated by identifying the positions of each of the 2^n different configurations of n bits in the input data string in accordance with the determined order. The control code and the position code are combined to form an encrypted data string.

Cellier et al. generally discloses a method and system for compressing and decompressing digital audio data. The digital audio data is first divided into a series of consecutive frames of data and each frame of data is further subdivided into a serial sequence of input data samples. Each frame of data is compressed individually.

Each input data sample is individually and sequentially supplied to a prediction filter. The prediction filter generates a predicted value for the received input data sample based on a history of previously received input data samples. The prediction filter compares the value of each received input data sample with the predicted value for that input data sample and generates a prediction error for each individual input data sample (See col. 3, lines 55-61). In this manner a prediction error is generated for each individual input data sample such that a set of prediction errors are generated for a serial sequence of input data samples within a frame.

The Cellier et al. method and system includes a plurality of Huffman tables. Each Huffman table includes 17 "bins" where each different bin represents a different range of error values based on a defined probability of the occurrence of that error value. For example, in one Huffman table, a first bin may be defined to include error values having a value of zero, a second bin may be defined to include error values having values of -1 and +1, a third bin may be defined to include error values having values of -3,-2, +2 and +3, etc. (See col. 6 lines 52-66). Each "bin" is assigned a unique prefix code. Each error value within each "bin" is assigned a unique suffix. (See col. 6 lines 45-49).

The best table selector retrieves the set of prediction errors associated with a serial sequence of input data samples associated with a specific frame of data. The best table selector identifies the Huffman table, which when used to encode the received set of prediction errors, will yield the most compact encoded representation. (See col. 4, lines 49-56) Each of the prediction errors for the frame of data is encoded using the corresponding suffix and prefix values from the identified Huffman table. A header is appended to the encoded data for the frame identifying the specific Huffman table used to encode the prediction error samples. (See col. 5, lines 1-10)

As can be seen, the Cellier et al. "position code" includes a prefix and a suffix where the prefix identifies a "bin" within a selected Huffman table and the suffix identifies the error value contained within the "bin" that corresponds to the magnitude of the prediction error. In contrast, the "position code," as recited in the claims at issue, refer to a position code that is generated by identifying the positions of each of 2^n different configurations of n bits in the input data string in accordance with a determined

order for querying the presence of each of 2^n different configurations of n bits within the input data string.

Furthermore, the order in which the queries are conducted in the invention recited by the claims at issue define the position code. Altering the order in which the queries are conducted alters the position code. While, Cellier et al. teaches querying a plurality of Huffman tables for the presence of the error values in the different bins, the order in which these queries are conducted have no impact on the compression of the input data. In other words, altering the order in which the Huffman tables or the bins are queried has no impact on the end result compressed version of the input data string. Since Cellier et al. does not disclose each of the elements recited by independent claim 1 and claims 2, 3, 5, 8-10, 47, 49-52, 53-55 and 59-61 dependent thereon, Applicant respectfully requests that the rejection of such claims as anticipated by Cellier et al. be withdrawn.

Turning now the rejection of independent claim 21 and claim 22 dependent thereon, as well as independent claim 23 and claims 24-26, 29-33, 35-37, 38-40 and 44-46 dependent thereon, as being unpatentable over Cellier et al. in view of the Schneier "Applied Cryptography" publication, the Schneier et al. article does not disclose or suggest Applicant's claimed invention. Schneier merely discloses that any encryption methodology can be implemented in software and does not disclose or suggest the above-described deficiencies of Cellier et al. Schneier does not disclose or suggest the implementation of any specific encryption methods or systems, let alone the methods and system for encrypting an input data string as recited by the claims at issue. Accordingly, Applicant respectfully requests that the rejection of independent claim 21 and claim 22

dependent thereon, as well as independent claim 23 and claims 24-26, 29-33, 35-37, 38-40 and 44-46 dependent thereon, be withdrawn.

Claims 6-7 stand rejected as unpatentable under 35 U.S.C. §103(a) as obvious over Cellier et al in view of Shimizu et al (U.S. Patent No. 6,772,343) and claims 27-28 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the combination of Cellier and Schneier and in view of Shimizu.

Claims 6-7 depend from independent claim 1 and therefore include the elements recited in independent claim 1 and claims 27-28 depend from independent claim 23 and therefore include the elements recited in independent claim 23. Applicant respectfully submits that the above-stated deficiencies of the disclosure of Cellier et al. with respect to independent claims 1 and 23 are not cured by the disclosure of Shimizu et al.

Shimizu et al. generally discloses a method and system for segmenting an input text string into a plurality of smaller blocks of data, dividing the segmented blocks of data into groups and encrypting the divided blocks of data using keys. A random number generator may be used to generate random numbers based on a seed retrieved from a seed storage device. The generated random number defines random block lengths for the segmented blocks.

Shimizu et al. does not disclose or suggest generating a position code by identifying the positions of each of 2^n different configurations of n bits in an input data string in accordance with a determined order for querying the presence of each of 2^n different configurations of n bits within the input data string as recited by the claims at issue. Accordingly, the rejection of claims 6-7 as being unpatentable over Cellier et al. in view of Shimizu et al should be withdrawn.

As mentioned previously, Schneier merely discloses that any encryption methodology can be implemented in software and does not disclose or suggest the above-described deficiencies of Cellier et al. Accordingly, the rejection of claims 27-28 as being unpatentable over the combination of Cellier et al. and Schneier and in view of Shimizu et al. should be withdrawn.

Claim 48 stands rejected under 35 U.S.C. §103(a) as unpatentable over Cellier et al. and in view of the Witten et al. "On the Privacy Afforded by Adaptive Text Compression" publication. Claim 34 stands rejected under 35 U.S.C. §103(a) as being unpatentable over the combination of Cellier et al., Schneier and Witten et al.

Claim 48 depends from independent claim 1 and therefore include the elements recited in independent claim 1. Claim 34 depends from independent claim 23 and therefore include the elements recited in independent claim 23. Applicant respectfully submits that the above-stated deficiencies of the disclosure of Cellier et al. with respect to independent claims 1 and 23 are not cured by the disclosure of Witten et al.

Witten et al. generally discloses an adaptive encryption method for transmitting secured communication of compressed data between parties by discouraging eavesdroppers who have not been listening since the very beginning of the transmission. Witten et al. falsely jumbles the frequency table (encoding/decoding table) used to compress the data. The jumbling "key" is produced by a random number generator based on a seed.

Witten et al. does not disclose or suggest generating a position code by identifying the positions of each of 2^n different configurations of n bits in an input data string in accordance with a determined order for querying the presence of each of 2^n different

configurations of n bits within the input data string as recited by the claims at issue Accordingly, the rejection of claim 48 as being unpatentable over Cellier et al. in view of Witten et al. should be withdrawn.

As mentioned previously, Schneier merely discloses that any encryption methodology can be implemented in software and does not disclose or suggest the above-described deficiencies of Cellier et al. Accordingly, the rejection of claim 34 as being unpatentable over the combination of Cellier et al. and Schneier and in view of Witten et al. should be withdrawn.

Claims 56-57 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cellier et al. in view of Weiss (U.S. Patent No. 5,479,512). Claims 41-42 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the combination of Cellier et al, Schneier and Weiss.

Claims 56-57 depend from independent claim 1 and therefore include the elements recited in independent claim 1. Claims 41-42 depend from independent claim 23 and therefore include the elements recited in independent claim 23. Applicant respectfully submits that the above-stated deficiencies of the disclosure of Cellier et al. with respect to independent claims 1 and 23 are not cured by the disclosure of Weiss.

While Weiss generally discloses a method and system for using an exclusive OR function to encrypt compressed data, Weiss does not disclose or suggest encrypting an input data string by generating a position code by identifying the positions of each of 2^n different configurations of n bits in an input data string in accordance with a determined order for querying the presence of each of 2^n different configurations of n bits within the

input data string as recited by the claims at issue Accordingly, the rejection of claims 56-57 as being unpatentable over Cellier et al. in view of Weiss should be withdrawn.

As mentioned previously, Schneier merely discloses that any encryption methodology can be implemented in software and does not disclose or suggest the above-described deficiencies of Cellier et al. Accordingly, the rejection of claims 41-42 as being unpatentable over the combination of Cellier et al. and Schneier and in view of Weiss should be withdrawn.

Claims 56 and 58 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cellier et al. in view of Butler et al. (U.S. Patent No. 5,861,887). Claims 41 and 43 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the combination of Cellier et. al., Schneier and Butler et al. (U.S. Patent No. 5,861,887).

Claims 56 and 58 depend from independent claim 1 and therefore include the elements recited in independent claim 1. Claims 41 and 43 depend from independent claim 23 and therefore include the elements recited in independent claim 23. Applicant respectfully submits that the above-stated deficiencies of the disclosure of Cellier et al. with respect to independent claims 1 and 23 are not cured by the disclosure of Butler et al.

Butler et al. generally discloses a method and system for iteratively reducing an image until the reduced image meets predefined size and resolution characteristics. Butler et al. does not disclose or suggest encrypting an input data string by generating a position code by identifying the positions of each of 2^n different configurations of n bits in an input data string in accordance with a determined order for querying the presence of each of 2^n different configurations of n bits within the input data string as recited by the

claims at issue Accordingly, the rejection of claims 56 and 58 as being unpatentable over Cellier et al. in view of Butler et al. should be withdrawn.

As mentioned previously, Schneier merely discloses that any encryption methodology can be implemented in software and does not disclose or suggest the above-described deficiencies of Cellier et al. Accordingly, the rejection of claims 41 and 43 as being unpatentable over the combination of Cellier et al. and Schneier and in view of Butler et al. should be withdrawn.

Since Cellier et al. standing alone does not disclose, and Scheier, Shimizu et al., Witten, Weiss or Butler in combination with Cellier et al. fail to disclose or even suggest the use of a encryption method and system that identifies the positions of each of 2^n different configurations of n bits in an input data string in accordance with a determined order for querying the presence of each of 2^n different configurations of n bits within the input data string as recited by the claims at issue, Applicant respectfully requests that the rejection of claims 1-3, 5-10 and 21-61 be withdrawn.

Since the prior art does not disclose each of the elements recited by the claims at issue, it follows that such claims are not anticipated thereby.

Furthermore, none of the prior art discloses or suggests that it would be desirable or even possible to use an encryption method and system that identifies the positions of each of 2^n different configurations of n bits in an input data string in accordance with a determined order for querying the presence of each of 2^n different configurations of n bits within the input data string as recited by the claims at issue. It is therefore evident that the claims are not obvious thereover. The prior art must disclose a suggestion of the incentive for the claimed combination of elements in order for a *prima facie* case of

obviousness to be established. See *In re Sernaker*, 217 U.S.P.Q. 1 (Fed. Cir. 1983) and *Ex Parte Clapp*, 227 U.S.P.Q. 972, 973 (Bd, Pat. App. 1985). Accordingly, Applicant respectfully requests that the Section 103(a) obviousness rejections also be withdrawn.

Claims 33, 42, 43, 57 and 58 have been amended to clarify the invention recited by such claims. No new subject matter has been introduced by way of such amendments.

For the foregoing reasons, reconsideration and withdrawal of the rejection of the claims at issue and allowance thereof are respectfully requested.

Respectfully submitted,

ICE MILLER

By: _____
Manisha Chakrabarti
Attorney No. 41665

ICE MILLER
One American Square, 31st Floor
Indianapolis, Indiana 46204
Telephone: (312) 726-8173
Facsimile: (312) 726-6254

Date: August 1, 2005

fig 2